

2/20/2008

DOCKET FILE COPY ORIGINAL

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

Received & Inspected

FEB 26 2008

FCC Mail Room

Re: EB Docket No. 06-36, Certification of CPNI Filing - Calendar Year 2007

Dear Ms. Dortch:

This letter serves as the below-named Company's "Certification of CPNI Filing for Calendar Year 2007", as ordered in EB Docket No. 06-36.

Company Name: Kasson & Mantorville Telephone Company

Address: 18 2nd Ave NW Kasson MN 55944

Form 499 Filer ID: 803727

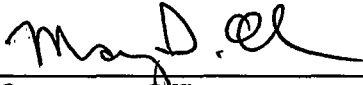
Name and Title of Signatory: Mary D. Ehmke COO/Secretary

I, Mary Ehmke, certify that I am an officer of the Company named above, and that, based on my personal knowledge and acting as an agent for the Company, the Company has established operating procedures that are adequate to ensure compliance with the rules established by the Federal Communications Commission ("FCC") concerning Customer Proprietary Network Information ("CPNI"), as set forth in Part 64, Subpart U, of the FCC's Rules and Regulations, 47 C.F.R. § 64.2001 *et seq.*, as revised.

The attached Statement demonstrates such compliance.

The Company [has/had not] taken any action (proceedings instituted or petitions filed by the Company at state commissions, the court system, or the FCC) against data brokers in the past year. [If yes, explain how pretexters are attempting to access CPNI and company actions and steps being taken to protect CPNI]

The Company [has/has not] received any customer complaints in the past year concerning unauthorized release of CPNI. [If yes, identify number and nature of complaint and breach, broken down by citatory of complaint]



Company Officer
Dated: 2/20/08

Attachment - Statement of Compliance

No. of Copies rec'd 0
List ABCDE

STATEMENT OF COMPLIANCE

The operating procedures of Kasson & Mantorville Telephone company ensure compliance with the FCC's CPNI Rules. Such procedures are as follows:

Use of CPNI in Marketing

Our company does not use CPNI in any of its marketing efforts, and does not permit the use of, or access to, customer CPNI by our affiliates or any third parties. We use, disclose or permit access to CPNI only for the purposes permitted under 47 U.S.C. Sections 222(c)(1) and (d).

Our company makes limited, one-time use of CPNI to market our communication-related services only in compliance with FCC Rule 64.2008.

Before (but proximate to) soliciting customer consent for the use of CPNI to market either (a) our (or our affiliates') communication-related services; or (b) third-parties' communication-related services, we give each customer notice of his or her right to restrict use and disclosure of, and access to, his or her CPNI, in compliance with FCC Rule 64.2008. Our company maintains a record of these notifications for at least one year.

Our company has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI. Each customer's record contains a designation identifying whether or not we have obtained, through the processes permitted by the FCC's rules, the customer's approval to use, disclose or permit access to his or her CPNI.

Our company accesses and uses a customer's CPNI to market our own (or our affiliates') communication-related services (outside a customer's current relationship) only after the customer's Opt-Out consent has been obtained in compliance with FCC Rule 64.2008, and which consent has not been revoked by the customer. Every two years our company (a) provides notice of customers' rights to restrict use and disclosure of, and access to, their CPNI, in compliance with FCC Rule 64.2008, and (b) solicits Opt Out consent for the use of the customer CPNI, in compliance with FCC Rule 64.2008, to each customer who has given Opt Out consent.

Our company permits access to and use of a customer's CPNI by third parties in order to market their communication-related services only after the customer's Opt-In consent has been obtained in compliance with FCC Rule 64.2008, and which consent has not been revoked by the customer.

Our company has a supervisory review process regarding our compliance with the FCC's CPNI rules for any outbound marketing efforts. We require sales personnel to obtain supervisory approval of any proposed outbound marketing request for customer approval.

CPNI Safeguards

Our company has designated a compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.

Our company trains its personnel as to when they are, and are not, authorized to use or disclose CPNI, and we have an express disciplinary process in place if the rules are violated.

Our company authenticates the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or in-store visit.

Our company discloses call detail information (CDI) in a customer-initiated call only: after the customer provides a pre-established password; or, at the customer's request, by sending the CDI to the customer's address of record; or by calling back the customer at his or her telephone number of record.

Our company discloses CPNI to a customer in person at our retail location(s) only when the customer presents a valid photo ID and the ID matches the name on the account.

Our company establishes passwords with customers in order to authenticate customers. Neither passwords nor the backup method for authentication rely on customers' readily available biographical information.

Our company has established password protection for customers' online accounts.

Our company notifies a customer immediately of changes in: a customer's password, a customer's response to back-up means of authentication, online account, or address of record.

CPNI Recordkeeping and Reporting

Our company maintains a record of our own and our affiliates' sales and marketing campaigns that use customer CPNI. We also maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. We maintain these records for at least one year.

Our company maintains records of our compliance with the FCC's CPNI Rules for use of CPNI in outbound marketing efforts, for at least one year.

Our company is prepared to provide the FCC with written notice, within five business days of any instance where the "opt out" mechanisms do not work properly.

Our company is prepared to notify the U.S. Secret Service and FBI within seven business days after the occurrence of an intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of CPNI. We may also notify the customer of such breach, after consulting with

the investigatory agency(ies), if we believe there is an extraordinarily urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. We will notify the customer of the breach after 7 business days following notification to the FBI and Secret Service, if such agencies have not requested that we postpone disclosure to the customer.

Our company will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.